SOA Runtime Governance

Mike Phillips
2011/11/08 15:15

Table of Contents

Purpose and Scope

The purpose of the SOA Runtime Governance Working Group is to establish the initial processes, roles and responsibilities for runtime governance. For our discussions, runtime governance includes the following:

- Access control
- Configuration changes, including version changes (deployment)
- Dependency tracking and notification
- Service interruptions

Stakeholders

1. **Technology Governance Board**
2. **CJIS - including county & local affiliates**
3. **Executive-Branch Agencies**
4. **Judicial Branch**
5. **DAS-ITE**
6. **ISO**

Use Cases / Scenarios

Web Proxy

Providing public/authorized access to a private web service

XML Firewall

Allows non-soap based services to protect themselves from common security threats.

Multi-protocol Gateway

Allows users to bridge protocols (HTTP/HTTPS/Stateless XML/Stateful XML)

Device Update/Patching

Updates to the firmware that may affect uptime and functionality.

Shared Resource Config

Resources that are shared across specific app domains (SSL cert, XSL file, etc.)

Troubleshooting

App Domain Creation

Initial setup of the app domain

Roles and Responsibilities

- **Application Owner -** The business owner of a specific application, which may be part of one or multiple app domains.
- **Governance Board** - The group charged with managing the runtime Governance process.
- **DP Root User** - Technicians with administrative access to the DataPower infrastructure devices.

- **Provider Point of Contact** - Person(s) who handle inquiries and requests for a given service.
- **Consumer Point of Contact** - Person(s) who respond to change requests and notifications for a given consumer of one or more service(s).

RACI Chart for SOA Governance

Task	App Owner	Governance Board	DP Root	Provider POC	Consumer POC	Comments
Initiate Change Request	A			R		
Send Change Notifications	A	I		R	I	
Approve Change Request	C	R, A	C	I	C	
Implement (Approved) Infrastructure Changes	I	A	R	C	I	Examples: • Create/ Delete App Domain • Grant/ Revoke initial App-Domain access • Deploy/ Roll Back device patch • Shut Down / Restart device(s) • Create/ Update shared resources (ports, etc.)
Implement (Approved) Provider Changes:	A	I	C	R	I	Examples: • Grant/ revoke App-Domain access • Set/ update App-Domain QoS limits • Create/ change conduit(s) to agency resources • Deploy/ update agency service(s)

- **Key:**
- **R/Responsible** - Individual(s) who perform a task; the doer, responsible for action/implementation. R's can be shared.

- **A/Accountable** - The individual who is ultimately accountable. Only one 'A' can be assigned to a task.
- **C/Consulted** - The individual(s) to be consulted prior to a final decision or actions taken. 2-way communication.
- **I/Informed** - The individual(s) who needs to be informed after a decision or action is taken.

Templates

- SOA Infrastructure SLA - The basic agreement between a providing agency and DAS-ITE that allows the agency to access the shared infrastructure.
- SOA Provider SLA - The agreement between each provider and consumer of a service that defines their roles and responsibilities to each other.

Parking Lot / Questions

1. Can we use LDAP to authenticate "box" users instead of local accounts? *No, you can use LDAP for service authentication but not to login to the datapower web interface.*
2. Does the yellow box do any protocol bridging (JMS)? *In addition to the support for HTTP/S and XML bridging there seem to be some hooks for FTP/NFS/IMS, CJIS is not using these features and is not familiar with the process for said features.*